ROUGH!

First DRAFT 5/10/2007
For submission to IAASS

Redefining Safety

Leonard B. Sirota, NASA

Abstract

NASA and the Aerospace community have traditionally included both risk to humans and hardware in the definition of "Safety". This leads to miscommunication with the public and can be an impediment to decision making. This paper offers two alternative approaches: first, applying the term "safety" only to humans and referring to the risk of damage or loss of hardware as an element of "mission success" and second, using different notation for each type of "safety".

Background

Merriam Websters Dictionary defines "safety" as: "The quality or condition of being safe; freedom from danger, injury, or damage; security."

Getting a little more specific, the Military Standard 882D Paragraph 3.2.10 defines safety as:
"Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment."

The current definitions for "safety" used by major space agencies of the world (Japanese, Canadian and European Space Agencies) are similar to the Military Standard above encompassing risks to human life, damage to or loss of flight or ground assets as well as risks to the environment.

The European Space Agency has a similar definition but adds even more specificity: Safety is:
System state where an acceptable level of risk with respect to:
- fatality,
- injury or occupational illness,
- damage to launcher hardware or launch site facilities,
- damage to an element of an interfacing manned flight system,
- the main functions of a flight system itself,
- pollution of the environment, atmosphere or outer space, and
- damage to public or private property is not exceeded

NASA's definition for safety goes even further talking about how you should measure and control safety risks. Safety. "Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. In a risk-informed context, safety is an overall mission and program condition that provides sufficient assurance that accidents will not result from the mission execution or program implementation, or, if they occur, their consequences will be mitigated. This assurance is established by means of the satisfaction of a combination of deterministic criteria and risk criteria."

Knowing that "Safety" has three major components we now look at how each is measured. When risk is evaluated, each of the three components have separate descriptions for each level of severity. Thus, as can be

seen in the ESA's table below for severity of consequences, loss of life, loss of systems, or loss of launch site facilities are all considered equally catastrophic.

In program management trade-offs are made to balance cost, schedule and technical risks. Within the range of "safety" there are similar trades to be made between those risks that affect mission success and the risks to life. By stating the severity of consequences ratings for each of the different risk categories the values for the trades are quantified. Thus, it is being demonstrated that the impact to a space agency is equal if you reduce the risk to a person from loss of life to temporary but not life threatening disability as it is to reduce the loss of launch site facilities to major damage to ground facilities.

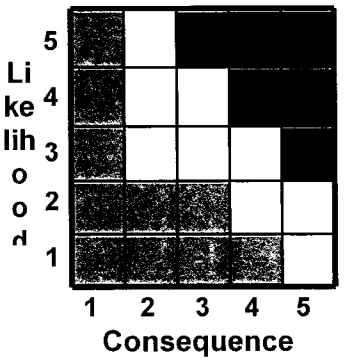
This aggregation of various risks within the same category leaves us with less than a precise understanding of the implications of these risks. Risks are rated by their potential consequences (hazards) and likelihood of occurrence. In order to communicate the level of risks within a program the risks are then plotted on a matrix where the highest consequence and likelihood risks are painted red, the lowest painted green with yellow for those in between. Each of the consequence levels are applied to all three types of "safety" with specific predetermined criteria. Several examples of these criteria are included in this paper. Looking at just the worst consequence, in the Space Shuttle Program loss of life, loss of program or catastrophic environmental impact are all at level "5". Each of these criteria are of extreme proportion and to be avoided. The European Space Agency (ESA) uses loss of life as the standard for humans and loss of launch site facilities for assets as the criteria for the highest consequence category. Since both human life and assets are parts of "safety" we come to the conclusion that loss of a launch facility is equal to loss of life. I contend that we do not see these as equal and would not be willing to consciously trade a life to save a launch pad, all other things being equal. In the decision process for flight operations we do whatever we can to save lives, regardless of the cost to assets. Thus, it is misleading to show both of these types of risks as equal and undistinguished risks on a safety risk matrix.

Then using only this definition for evaluating risks it appears that we equate loss of life with loss of an specified dollar value of ground support equipment. Clearly we do not make such trades but, we need to use better tools to communicate the fact that these are two different categories of risk requiring separate evaluation. Therefore, I am proposing that, when talking about safety risks we clarify our meaning by separating the safety risks into three categories: risks to human life (S_H), risk to flight or ground assets (S_A), or risk to the environment (S_E). This permits us to better understand and communicate the rationale and impact of risk decisions. In this paper we will primarily address the S_H and the S_A.

NASA performs a Safety and Mission Success Review prior to all significant NASA launches. The central feature of these reviews is an assessment of risks to safety and mission success as displayed on a matrices with the variables on the axes: Consequence and Likelihood. The Consequences for the safety matrix are based on the definition of "Safety" as follows:

Space Shuttle Program Risk Management Scorecard

Likelihood	
5	**Very Likely: ~10^{-1}** Expected to happen.
4	**Likely: ~10^{-2}** Could happen. Controls have significant limitations or uncertainties.
3	**Possible: ~10^{-3}** Could happen. Controls exist with some limitations or uncertainties.
2	**Unlikely: ~10^{-4}** Not expected to happen. Controls have minor limitations or uncertainties.
1	**Highly Unlikely: ~10^{-5}** Extremely remote possibility that it will happen. Strong controls in place.



Identify and Assess Risk

- **Start with a Concern.** Is this a program risk?
  - What information is available? Gather information: requirements status, problem data, trends, hazards, critical item history, etc.
- **Define Risk Statement.**
  - Given the condition _(A)_ , there is a possibility that _(B)_ will occur.
    (A) - Single phrase briefly describing current key circumstances or situations that are causing concern, doubt, anxiety, or uncertainty
    (B) - Consequences or impacts of the current conditions that could be realized due to (A)
- **Define the Consequences (B).** Locate the most accurate description(s) among the Safety, Mission Success, Supportability, Cost, and Schedule consequence descriptions.
- **How likely is this risk scenario?** Likelihood is the chance of a risk occurring.
  - Evaluating the likelihood rating requires subjective judgment. Select the most accurate rating based on the quantitative values **or** the qualitative descriptions.
  - Only one rating is selected per risk statement. It is evaluated for the period being assessed.
- **Plot the Risk.** Select the highest consequence score. Plot this against the ONE Likelihood Score on the RED/YELLOW/GREEN risk matrix.

Consequence			1	2	3	4	5
TECHN	Safet	*Human Health*	- Minor or first aid Injury	- Moderate injury, illness, incapacitation or impairment	- Significant or long-term injury, illness, incapacitation or impairment	- Permanent or major injury, illness, incapacitation or impairment	- Death
		System Safety	- Damage to non-flight Critical assets	- Loss of non-flight critical assets	- Damage to major element(s) of flight vehicle or ground facility	- Loss of major element(s) of flight vehicle or ground facility	- Loss of program
		Environmental Safety	- Minor environmental impact	- Moderate environmental impact	- Significant environmental Impact	- Major environmental impact	- Catastrophic environmental impact
		HSE Compliance	- Minor non-compliance	- Moderate non-compliance	- Significant non-compliance	- Major non-compliance	- None defined
	Mission Succes	*Shuttle Operations*	- Minor increase in flight operations timelines or complexity	- Failure to achieve any planned SSP mission objective	- Minimum duration flight (MDF) - Significant increase in flight operations timelines or complexity	- Failure to achieve all Shuttle major mission objectives (MMO) - Early mission termination - Pad abort or intact abort	- Contingency abort - Shuttle crew evacuation
		ISS Operations	- None defined	- Failure to achieve any planned ISS mission objective	- None defined	- Failure to support assembly critical ISS requirements	- ISS evacuation
		SSP Developmental Activities	- Failure to meet developmental requirements, minor workarounds or temporary waivers required for flight	- None defined	- Inability to complete commit to flight test, analysis or certification - Failure to meet developmental requirements. Significant or permanent waivers required for flight	- Failure to meet key development requirements (e.g. performance)	- None defined
	Supportability	*Capability to Maintain SSP Assets*	- Temporary usage loss or LOCM of non-flight critical asset	- Permanent usage loss or LOCM of non-flight critical asset	- Temporary usage loss or LOCM of major element(s) of flight vehicle or ground facility	- Permanent usage loss or LOCM of major element(s) of flight vehicle or ground facility	- Inability to support further Shuttle flight operations
		Flight Processing	- Collateral damage to non-flight critical assets during processing	- Moderate increase timeline or complexity	- Collateral damage to major element(s) of flight vehicle or ground facility during processing - Significant increase timeline or complexity	- Loss of major element(s) of flight vehicle or ground facility due to direct or collateral damage during processing	- None defined
PROGRAM	Schedul	*SSP / ISS Schedule*	- Minor operational slips	- Less than 7-day slip in an SSP/ISS freeze point or milestone	- Greater than 7-day slip in an SSP/ISS freeze point or milestone - ISS hardware/software delivery date not met for on-orbit needs	- One flight decrease from baselined manifest - One mission increase in ISS assembly plan - Flight delay occurring pre-FRR - SSP/ISS milestone slip of more than one month	- Two or more flight decrease from baselined manifest - Two or more mission increase in ISS assembly plan - Flight delay after L-2 - Cannot achieve major SSP/ISSP milestone
	Cos	*Risk Recovery Cost*	< $1 M	$1 M - $5 M	$5 M - $15 M	$15 M - $25 M	> $ 25 M

Reference NSTS 07700, Volume XIX

The European Space Agency uses the following criteria to rate the severity of consequences:

The severity of potential consequences of identified hazardous events shall be categorized as shown in Table 1:

Table 1: Severity of consequences

Severity	Level	Dependability	Safety
Catastrophic	1	---	Loss of life, life-threatening or permanently disabling injury or occupational illness;
			Loss of system;
			Loss of an interfacing manned flight system;
			Loss of launch site facilities;
			Severe detrimental environmental effects.
Critical	2	Complete loss of mission	Temporarily disabling but not life-threatening injury, or temporary occupational illness;
			Major damage to interfacing flight system;
			Major damage to ground facilities;
			Major damage to public or private property;
			Major detrimental environmental effects.
Major	3	Major mission degradation	---
Minor or Negligible	4	Minor mission degradation or any other effect	---
Note: The			

severity category is the highest severity category of the function associated with the system or system component.			

Again, these two tables reflect a very similar view in favor of aggregating the various aspects of safety.

It is my contention that the safety risk trade above is not equal and should not be shown as equal on the same risk matrix without clearly identifying which type of risk is being shown. With equal likelihood, a potentially catastrophic risk to facilities or flight hardware may be acceptable for launch and the decision reasonably straight forward, but a potentially catastrophic risk to humans would be a more difficult decision to make harder to accept and even harder to explain to the public. Therefore, we need to always be clear about what type of safety risk we are evaluating and portraying.

Impact of Current Definition on Decision Process and Communication

We have risk matrices that show relative magnitude and ranking of safety risks. We use this tool in program reviews and as an aid to program management to focus on the most critical issues. When we lump together risks to assets with risks to humans on the same matrix without discriminating notations we are oversimplifying the circumstances and complicating the decision process. Although a risk to flight crew and a risk to ground support equipment may have the same rating on the safety matrix our reaction to them is not equal. Clearly we hold the value of life to be higher than hardware assets and will make decisions with this in mind.

An example to clarify the point:

Before the Shuttle STS-114 launch it was determined that due to debris concerns the risk for the mission was considered to be "red". This was based on the concern for loss of the Orbiter. For this reason the NASA Chief, Safety and Mission Assurance and the NASA Chief Engineer voted not to launch. This recommendation was overridden by the NASA Administrator because there were really two risks imbedded in the one point on the matrix. First there was the risk to the flight hardware which could suffer a catastrophic event due to damage incurred on ascent. The second risk was to the crew. Because there was a plan in place to support the crew on the International Space Station until a Launch on Need rescue vehicle could launched to return them to Earth their risk was in the "yellow". With this rationale the Chief, SMA and the Chief Engineer chose not to take a dissenting opinion forward again.

Despite the reasonable rationale for the decision it was difficult to communicate to the public because all they saw was a "red" for safety.

Currently Used Alternative Approach

The International Space Station (ISS) program uses different scales for rating risk depending on the application. I would like to call your attention to the risk rating card (chart x below) which is used to compare the relative risks for the overall program. In this instance the definition used for safety risks relate only to human life. All impacts to flight systems are considered Mission Success risks. With this narrow focus for "safety" it is now easier to rapidly distinguish the risks and impacts of decision on humans versus hardware.

Analysis

Currently the different types of safety risks, each measured with a different set of criteria, are placed on the same matrix without clearly indicating which scale was the basis for the evaluation (see table ---------- taken from NPR ----------). The ones associated with assets only affect cost, schedule and mission success which do not directly impact human life. The second category, risks to the environment also may affect cost, schedule and mission success but, can, to varying degrees; have an impact on humans beyond the scope of the mission but, short of directly and immediately impacting human life.

There is little risk of choosing the wrong course of action due to the aggregation of the different types of risk on the same matrix. Decisions for action are not based solely on a risk matrix but with careful review analysis and understanding of the technical basis for the risks and the impact of each possible option.

The risks are in communication to the public and to other members of the aerospace community where little supporting detail comes with the graphic representations of risk. They only see the "X" for safety in the red box.

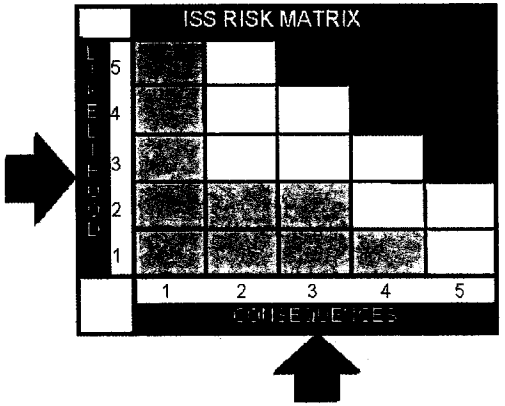
There are several options available to improve our communication.

1. Leave the matrices and rating systems as they are but be more aware of the need to differentiate between risks to human safety versus assets or environmental safety. When speaking about these risks always clarify what is at risk. In this option the matrices do not speak for themselves and must be accompanied by verbal or written narrative giving further explanation of the risk ratings.
2. Always use a separate matrix to display risks to humans. There is little room for misinterpretation with this option, but it does add more individual matrices to any evaluation of risks and, based on the more commonly used broader definition of "safety", it makes it more difficult to get a quick snapshot of all the most critical issues that need to be addressed.
3. Use subscripts to identify the various types of risks portrayed on the matrix (S_H, S_A, S_E). This approach captures the important distinction between the various types of "safety" risk in the same simple matrix format while still displaying all the various "safety' risks on the same page. The only minor downside to this approach is the addition of more detail to what may be an already cluttered chart.

It is always going to be necessary for people dealing with these risks and communicating them to each other and the public to be clear about what types of risk are being discussed. But, this is not sufficient. The charts that are presented and the records maintained for aerospace activities need to reflect these distinctions and not solely rely on the oral presentation to convey the differences in these safety risks. Either option two or three above can be made to work

ISS PROGRAM RISK SCORECARD

Likelihood Rating		
5	Very Likely	Expected to happen in the life of the program Controls are missing or insufficient
4	Likely	Likely to happen in the life of the program Controls have significant limitations or uncertainty
3	Possible	Could happen in the life of the program Controls exist, with some limitations or uncertainty
2	Unlikely	Unlikely to happen in the life of the program Controls have minor limitations or uncertainty
1	Highly Unlikely	Extremely remote possibility that it will happen in the life of the program Strong controls in place



Mitigation

- High – Implement new process(es) or change baseline plan(s)
- Medium – Aggressively manage; consider alternative process
- Low – Manage within normal processes; monitor

Consequence Rating	1	2	3	4	5
Mission Success / Operational Performance	Minor or no impact to mission objectives Nominal Execution of Mission Minor reduction in performance Minor or no impact to design or operating margins	Failure to meet any single mission objective Operating in a degraded state Moderate reduction in performance Can handle within design or operating margins Damage to non-critical system, element, ground facility, function, or emergency system	Significant impact to mission objectives Operational Workarounds available Significant reduction in performance Significant loss of design or operating margin Loss of any non-critical system, element, ground facility, or function Loss of emergency system	Loss of multiple mission objectives Major increase in flight operations timelines or complexity Major degradation in performance Loss of all design or operating margin Damage to critical system, element, ground facility, or function Planned De-Crewing	Loss of entire mission No alternatives exist Loss of ISS or any critical system, element, major ground facility or function ISS in a condition which prevents rendezvous/docking operations Emergency Evacuation
Safety	No injury	Minor injury, minor illness	Significant or long-term injury, illness, incapacitation or impairment Non-disabling injury	Permanent injury, impairment or incapacitation	Loss of Life Disabling injury
Cost - Score by cost of mitigating risk	Minimal impact (<$100K) or 0 to 2.5% increase	Moderate impact ($100K up to $1M) or 2.5% to 5% increase	Significant impact ($1M up to $10M) or 5% to 7.5% increase	Major impact ($10M up to $50M) Or 7.5% to 10% increase	Major impact (> $50M) Or >10% increase
Schedule	Minor or no impact	Can handle with schedule reserve, no impact to key project milestone or critical path	Project milestone slip No impact to Program critical path	Impact to Program milestone and/or Program critical path	Cannot meet program critical path milestone(s)

Note: Risk management is a communication system where a *qualitative* score can help in understanding of a risk. This card is only a rough guide for determining a likelihood and consequence for a risk. Significant resources should not be spent scoring a risk. Score is relative to the risk's highest elevation; i.e. sub-org, Org, or Top Program Risk.

References

NASA NPR 8715.3A NASA General Safety Program Requirements - **APPENDIX B. Glossary of Safety and Risk Management Terms**

SSP 50175 Rev B Annex. A Page 1 of 2

Webster's New twentieth Century Dictionary of the English Language Unabridged – second edition – 1955